APPENDIX B

IPSec, VPN, and Firewall Concepts

This appendix introduces the concepts of Internet Security Protocol (IPSec), virtual private networks (VPNs), and firewalls, as they apply to monitoring with Performance Monitor:

- Overview: IPSec and Related Concepts, page B-1
- Overview: VPN Concepts, page B-4
- Overview: Firewall Concepts, page B-10
- Additional Terms, page B-13

Overview: IPSec and Related Concepts

The IPSec framework is a set of open standards developed by the Internet Engineering Task Force (IETF). This framework provides cryptographic security services at Layer 3, the Network layer of the OSI model.

The following topics describe essential aspects of IPSec.

- Understanding the IPSec Framework, page B-2
- Understanding Layer 2 Protocols, page B-3

Understanding the IPSec Framework

The IPSec framework provides these essential features for secure communication:

- Peer authentication
- Data confidentiality
- Data integrity
- Data origin authentication

The IPSec framework facilitates these features with two types of tunnels:

- Key management tunnels—also known as Phase-1 (IKE) tunnels.
- Data management tunnels—also known as Phase-2 (IPSec) tunnels.

Key management tunnels and data management tunnels both require security associations.

Understanding Layer 2 Protocols

There are three types of Layer 2 protocols: PPTP, L2F, and L2TP.

Table B-1 Layer 2 Protocols

Protocol	Description
L2F	Layer 2 Forwarding (L2F) creates Network Access Server (NAS)-initiated tunnels by forwarding Point-to-Point (PPP) sessions from one endpoint to another across a shared network infrastructure. Cisco Systems developed the L2F protocol.
L2TP	Layer 2 Tunneling Protocol (L2TP) is an IETF standard tunneling protocol that tunnels PPP traffic over LANs or public networks. L2TP was developed to address the limitations of IPSec for client-to-gateway and gateway-to-gateway configuration, without limiting multivendor interoperability. An extension of PPP, L2TP is based on L2F and PPTP.
PPTP	Point-to-Point Tunneling Protocol (PPTP) is not a standard tunneling protocol. Microsoft developed PPTP, which—like L2TP—tunnels Layer 2 PPP traffic over LANs or public networks. PPTP creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over the Internet or other TCP/IP-based networks.

Overview: VPN Concepts

A virtual private network (VPN) is a framework that consists of multiple remote peers transmitting private data securely to one another over an otherwise public infrastructure (generally a shared IP backbone), such as the Internet. In this framework, inbound and outbound network traffic is protected by using tunnels that encrypt all data at the IP level. The framework permits networks to extend beyond their local topologies while providing remote users with the appearance and features of a direct network connection.

Typically, remote peers (sites and users) are connected to the central site over a shared infrastructure in a hub-and-spoke topology, although it is possible to configure remote access VPNs in two other ways. These other configurations are called “full mesh” and “partial mesh.” Performance Monitor supports all of these VPN types.

Key Terms and Acronyms in VPN Technologies

These terms and acronyms might help you improve your understanding of general VPN technologies.

Acronym	Term	Definition
3DES	Triple Data Encryption Standard	A data encryption standard that applies three 56-bit private keys in succession to 64-byte blocks of data. US only.
AH	Authentication Header	A component of IPSec packets that provides basic data authentication.
CA	Certification Authority	An agency that provides digital certificates that its clients can use to establish or prove their identity to peers and secure their communications.
CBC	Cipher Block Chaining	A cryptographic mode that provides data encryption and authentication using AH and ESP.
DES	Data Encryption Standard	A standard method of data encryption that applies 56-bit private keys to 64-byte blocks of data.
DH	Diffie-Hellman Key Exchange	A protocol that enables two devices to exchange keys securely over an insecure medium.

Acronym	Term	Definition
ESP	Encapsulating Security Protocol	A protocol that provides tunneling services for encryption and/or authentication.
HMAC	Hashed Message Authentication Code	A technique that provides message authentication using hashes for encryption.
IETF	Internet Engineering Task Force	Task force responsible for developing Internet standards.
IKE	Internet Key Exchange	A control protocol that negotiates, establishes, maintains, and tears down IPSec connections.
IPSec	IP Security Protocol	A framework of open standards that provides data confidentiality, data integrity, and data origin authentication between peers that are connected over unprotected networks such as the Internet. IPSec provides security services at the IP layer and can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. IPSec acts at the network layer to protect and authenticate IP packets, while offering three methods of authentication: preshared keys, digital certificates, and RSA encrypted nonces.
ISAKMP	Internet Security Association and Key Management Protocol	A generic protocol that enables two devices to exchange security parameters.
L2F	Layer 2 Forwarding	A tunneling protocol that creates network access server (NAS)-initiated tunnels for forwarding PPP sessions.
L2TP	Layer 2 Tunneling Protocol	An IETF standard tunneling protocol for VPNs, designed to tunnel PPP traffic over LANs or public networks.
LAC	L2TP Access Concentrator	Device terminating calls to remote systems and tunneling PPP sessions between remote systems and the LNS.
LNS	L2TP Network Server	Device able to terminate L2TP tunnels from a LAC and terminate PPP sessions to remote systems through L2TP data sessions.
MAC	Message Authentication Code	The cryptographic checksum of the message used to verify its (the message's) authenticity.

Acronym	Term	Definition
MD5	Message Digest 5	The result of a computation that provides basic message authentication.
NAS	Network Access Server	Gateway that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs both synchronous and asynchronous routing of supported protocols.
PAC	PPTP Access Concentrator	Device terminating calls to remote systems and tunnelling PPP sessions between remote systems and the PNS.
PNS	PPTP Network Server	Device able to terminate PPTP tunnels from a PAC and terminate PPP sessions to remote systems through PPTP data sessions.
PPP	Point-to-Point Protocol	A protocol that tunnels multiple network-layer protocols.
PPTP	Point-to-Point Tunneling Protocol	A Microsoft protocol for Layer 2 that serves the same purpose as L2TP.
PSTN	Public Switched Telephone Network	Any of a variety of telephone networks and services in place worldwide. Also called Plain Old Telephone System (POTS).
SA	Security Association	A set of security parameters that defines a particular tunnel. Key management tunnels employ one SA, while data management tunnels employ at least two.
SHA	Secure Hash Algorithm	An algorithm that provides strong message authentication.
SPI	Security Parameter Index	A number that, together with a destination IP address and security protocol, uniquely identifies a particular security association.
VPN	Virtual Private Network	A secure communication channel that provides the same network connectivity for remote users over a public infrastructure as they would have locally in a private network.

Understanding Types of VPNs

A VPN provides the same network connectivity for remote users over a public infrastructure as they would have over a private network. VPN services for network connectivity consist of authentication, data integrity, and encryption.

The two basic VPN types are remote access and site-to-site. See Table B-2.

Table B-2 Basic VPN Types

VPN Type	Description
Remote Access	Remote access VPNs secure connections for remote users, such as mobile users or telecommuters, to corporate LANs over shared service provider networks. There are two types of remote access VPNs: • Client-Initiated. Remote users use clients to establish a secure tunnel through a shared network to the enterprise. • NAS-Initiated. Remote users dial in to an ISP Network Access Server (NAS). The NAS establishes a secure tunnel to the enterprise private network that might support multiple remote user-initiated sessions.
Site-to-Site	The two common types of site-to-site VPNs (also known as LAN-to-LAN VPNs) are intranet and extranet. Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a public infrastructure. Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a public infrastructure.

Understanding VPN Components

The three main components of VPNs are tunnels, endpoints, and sessions. See Table B-3.

Table B-3 Primary VPN Components

Component	Description
Tunnels	Virtual channels through a shared medium. They provide a secure communications path (an encapsulated traffic flow) between two peers. Every VPN tunnel can consist of multiple sessions.
Endpoints	A network device on which a tunnel ends. The following devices can serve as endpoints: a computer running a VPN client, a router, a gateway, or a network access server. The two ends of a tunnel are commonly called the source and the destination endpoints. • A source endpoint initiates the tunnel. • A destination endpoint terminates the tunnel.
Sessions	Portions of tunnels that pertain to the transmission of a specific user in a single, tunneled PPP call between two peers. A remote access tunnel can contain one or more PPP connections. Each connection represents one user. However, Performance Monitor refers to *any* user connection to a device as a session.

Understanding VPN Services

VPNs provide four types of services: peer authentication, data confidentiality, data integrity, and data origin authentication.

Table B-4 Services that VPNs Provide

Service	Description
Peer authentication	Endpoints verify each other's identity before establishing a VPN tunnel.
Data confidentiality	Endpoints use encryption to prevent the unauthorized viewing of transmitted packets.
Data integrity	Destination endpoint confirms that packets received from the source endpoint are identical to the packets that were transmitted.
Data origin authentication	Destination endpoint confirms that received data originated from the source endpoint.

Understanding VPN Tunnels

The following topics explain the function and structure of VPN tunnels.

- Understanding Key Management Tunnels, page B-9
- Understanding Data Management Tunnels, page B-10
- Understanding Security Associations, page B-10

Understanding Key Management Tunnels

Key management tunnels (also called Phase-1 or IKE tunnels) set up and maintain data management tunnels. Key management tunnels use the IKE protocol to perform their functions. The IKE protocol authenticates the peer and then negotiates a compatible security policy before establishing the data tunnel.

The key management tunnel facilitates:

- IPSec Key Negotiation.
- IPSec Key Renegotiation.
- The exchange of control messages for maintaining data management tunnels.

Understanding Data Management Tunnels

Data management tunnels (also called Phase-2 or IPSec tunnels) secure data traffic. Data management tunnels use the Authentication Header (AH) protocol and the Encapsulated Security Protocol (ESP) to perform their operations.

Data management tunnels facilitate:

- Data integrity.
- Data confidentiality.

Data management tunnels can be set up automatically by using key management tunnels or manually by operators.

The two modes of operation for a data management tunnel are:

- Tunnel mode, in which the tunnel protects both the data and the identities of the endpoints.
- Transport mode, in which the tunnel protects only the data.

Understanding Security Associations

A security association (SA) is a set of security parameters for authentication and encryption used by a tunnel. Key management tunnels use one SA for both directions of traffic; data management tunnels use at least one SA for each direction of traffic. Each endpoint assigns a unique identifier, called a security parameter index (SPI), to each SA.

Overview: Firewall Concepts

A firewall is a router, an access server, or a service module (or several such devices), designated as a buffer between any connected public networks and a private network. A firewall uses access lists and other methods to ensure the security of the private network.

Performance Monitor monitors firewall services that originate on either of two different kinds of Cisco devices:

- PIX 500 Series Firewalls, page B-11
- Firewall Service Modules, page B-11

PIX 500 Series Firewalls

PIX 500 Series Firewalls are Cisco appliances that use the PIX OS to provide:

- AAA (RADIUS/TACACS+).
- Content (Java/ActiveX) filtering and URL filtering.
- DHCP client/server.
- Intrusion protection.
- Network Address Translation (NAT) and Port Address Translation (PAT).
- Point-to-point protocol over Ethernet (PPPoE) support.
- Standards-based IPsec VPN.
- Stateful inspection firewalling.
- X.509 PKI support.

PIX Firewalls also provide security services for multimedia applications and protocols including Voice over IP (VoIP), H.323, SIP, Skinny Client Control Protocol (which is a Cisco-developed replacement for the H.323 protocol), and Microsoft NetMeeting.

Firewall Service Modules

A firewall service module is a multigigabit, fabric-enabled module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers. It is deployed at the enterprise campus edge and at distribution points.

Note Performance Monitor monitors firewall service modules only when they are installed in a Catalyst 6500 switch. Routers in the Cisco 7600 Series are not supported in this Performance Monitor release. See *Supported Devices and Software Versions for Monitoring Center for Performance 2.0*.

A firewall service module has no external ports. Instead, it allows any port on a Catalyst 6500 chassis to operate as a firewall port. It uses the Cisco PIX operating system to provide:

- High-performance (5 Gbps), full-duplex firewall functionality.
- 3M pps throughput.
- Support for 100 VLANs.
- 1M concurrent connections (setup rate of 100,000 connections per second).
- LAN failover: active/standby, inter/intra chassis.
- Dynamic routing with OSPF/RIP.
- Up to 4 modules per chassis (scalable to 20 GB per chassis).
- Cut-through proxies enforce security policies per VLAN.
- The complete feature set of Cisco PIX 6.0 software and these features of the Cisco PIX 6.2 software:
  - Command authorization.
  - Object grouping.
  - ILS/NetMapping fixup.
  - URL filtering enhancement.

Additional Terms

Familiarity with these terms will help you to understand the Performance Monitor application and its associated technologies.

Term	Definition
alarm	An alarm signifies abnormal operation in a service, a network entity, or a part of a network entity.
alert	Alarm (audible or visual) that signals an error or serves as a warning.
authentication	In a VPN, the verification of peer identity using any combination of device authentication, data origin authentication, extended authentication, and data integrity checking. In the context of AAA, entity authentication is the method of verifying user ID, including login and password, challenge and response, messaging support, and—depending on the security protocol that is selected—encryption.
authentication method	One of several procedures for verifying the identity of a peer, such as a challenge password or a digital certificate.
community string	Text string that authenticates the issuer of an SNMP query.
CSV file (Comma-Separated Value)	A common text file format that contains comma-delimited values. In the case of Performance Monitor, these values describe devices and their attributes.
device	In Performance Monitor, a device is either a physical node in the network or it is a virtual node that is defined by a physical node. In either case, whether physical or virtual, a device must be IP-addressable.
device hierarchy	Levels in which devices are grouped in an Object Selector. All devices are categorized into groups.
event	An event is a notification that a managed device or component has an abnormal condition. Multiple events can occur simultaneously on a single monitored device or service module. To display events, you open an Event Browser.
event logging	A mechanism by which events are archived and collected for viewing.
firewall	A device that provides firewall services. In Performance Monitor, a firewall is a PIX firewall appliance or a firewall service module for a Catalyst Series switch.

Term	Definition
group	A device group in Performance Monitor is a collection of devices (or groups of devices) that is the equivalent of a folder, offering an organizational convenience. Some groups are system-defined and others are user-defined. Among the devices in a user-defined group, no physical, logical, or topological relationship is assumed unless you organize devices in a consistent way. In a broader sense, a group is any collection of network objects, devices, users, or other entities for which rules can be defined.
importing devices	Importing is a mechanism by which you transfer a descriptive list of device attributes from an outside inventory to Performance Monitor. Supported import sources are Resource Manager Essentials (RME), Management Center for VPN Routers (Router MC), or a comma-separated value (CSV) file.
inbound	Traffic that a device receives through its interfaces.
interface	A physical or logical subcomponent through which a device can connect to other devices.
IPSec tunnel	An IPSec tunnel is a tunnel established between two peers and secured with IPSec protocols.
LAN-to-LAN VPN	See site-to-site VPN.
load balancing	A mechanism that distributes incoming service requests evenly among servers in the back end, such that the load distribution is transparent to users.
outbound	Traffic that a device transmits through its interfaces.
SNMP (Simple Network Management Protocol)	Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SNMP trap	A notification event issued by a managed device to the network management station when a significant event (not necessarily an outage, a fault, or a security violation) occurs.
SSL (Secure Sockets Layer)	Encryption technology for the web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
threshold	Value, either upper- or lower-bound, that defines the maximum or minimum allowable condition before an alarm is sent.
unmanaged	An unmanaged device in Performance Monitor is known, but not polled.